

Honorable John C. Coughenour

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

UNITED STATES OF AMERICA,

Plaintiff,

v.

JOSEPH SAM a/k/a WILLIAM
EARLYSTAR CLARK,

Defendant.

NO. CR19-115-JCC

UNITED STATES' OPPOSITION TO
DEFENDANT'S MOTION TO SUPPRESS
CELL PHONE CONTENTS

Noted on Motion Calendar: March 27, 2020

The United States of America, by and through Brian T. Moran, United States Attorney for the Western District of Washington, and Rebecca S. Cohen and J. Tate London, Assistant United States Attorneys for said District, files this response in opposition to the Motion to Suppress Cell Phone Contents filed by Defendant Joseph Sam (Docket No. 55). The Government asks the Court to deny Sam's motion because the officers' actions in this case do not constitute the type of warrantless search for cell phone data prohibited by *Riley v. California*, 573 U.S. 373 (2014). Officers did not impermissibly search the phone. Instead, they simply touched the power button on the phone to wake it up, which resulted in the display of the public-facing lock-screen wallpaper, an image not even protected by the lock on the phone. It is the information displayed in the lock screen that Sam seeks to suppress,

1 but the relevant name displayed on the image is not “cell phone data” that requires a warrant
2 in order to search.

3 **I. BACKGROUND**

4 Defendant Joseph Sam is charged in a three-count Indictment with (1) Conspiracy to
5 Commit Robbery, in violation of Title 18, United States Code, Section 371; (2) Robbery, in
6 violation of Title 18, United States Code, Sections 2, 1153 and 2111; and (3) Assault
7 Resulting in Serious Bodily, in violation of Title 18, United States Code, Sections 1153(a)
8 and 113(a)(6). The charges arise from a robbery that occurred at a residence on the Tulalip
9 Indian Reservation on February 6, 2019, in which the government alleges that Sam, co-
10 defendant Dennis Peltier, and unindicted co-conspirator Mariah Bourdieu conspired to rob –
11 and did in fact rob – victim John Doe of approximately one ounce of heroin. The
12 government also alleges that during the course of the robbery, Sam shot John Doe in the
13 back, causing a spinal cord injury and paralysis to his lower body.

14 Law enforcement identified and arrested co-defendant Peltier and unindicted co-
15 conspirator Bourdieu within days of the robbery and shooting. It took longer for law
16 enforcement to identify Sam because at the beginning of the investigation all they had to go
17 on for the identity of the shooter was his nickname, “Strap.” Law enforcement later
18 identified Sam as “Strap,” in part due to conversations found on Bourdieu’s Facebook
19 account with a Facebook user by the Facebook name of “Streezy NW,” who Bourdieu
20 referred to in messages as “Strap.”

21 On May 15, 2019, Sam was arrested on an arrest warrant issued by the Tulalip Tribal
22 Court, and searched incident to arrest, when a cell phone was recovered from his person.
23 Later that day, pursuant to inventory procedures, officers examined the phone to determine
24 the type of phone and whether it was locked, and to place it into airplane mode so the phone
25 could not be wiped remotely. In doing so, officers saw that the lock screen identified the
26 provider as “Metro PCS” and displayed the name “STREEZY” under the time and date.
27 Dkt. 55-1, at page 3 (1st paragraph). Officers then placed the phone in airplane mode to
28 prevent remote wiping. In February of 2020, the FBI again pressed the power button to

bring the phone out of sleep mode, and then reviewed the lock screen and took a picture of it. The picture shows the nickname “STREEZY” on the lock screen, under the displayed time and date, just as officers had originally viewed in May of 2019. Dkt. 55-2.

In December of 2019, co-defendant Peltier pleaded guilty to Count 1 (Conspiracy to Commit Robbery) and Count 2 (Robbery) in the Indictment. He has not yet been sentenced. Because she is not an enrolled member of a federally recognized tribe like Sam and Peltier, co-conspirator Bourdieu was charged in Snohomish County Superior Court, and is awaiting trial.

Sam has now filed a Motion to Suppress Cell Phone Contents (Dkt. 55), arguing that the contents of the phone’s lock screen must be suppressed because law enforcement viewed the lock screen and took a picture of it without a warrant. For the reasons discussed below, the government asks the Court to reject Sam’s argument and deny the motion.

II. ANALYSIS AND ARGUMENT

A. Sam Had No Reasonable Expectation of Privacy in a Lock Screen that He Programed to Have the Banner Read “STREEZY.”

Sam’s motion deals with the digital “lock screen” of his Android phone. A lock screen of a phone is a public-facing screen that can be viewed when someone touches or otherwise activates a phone. Because the phone remains locked, the phone’s data generally cannot be accessed from the lock screen.

A lock screen is customizable, and the user of a phone can choose what pictures, wallpaper, or other information is displayed to the public from the lock screen. Often times, individuals will choose to put their name on the lock screen so that they can be identified in the event that a phone is misplaced or mistaken for someone else’s phone. Here, Sam specifically designed his lock screen to display the nickname “STREEZY” to anyone who activated the phone and/or viewed the lock screen. He cannot now claim that he has a privacy interest in what he deliberately chose to display to the public.

B. Law Enforcement Did Not Search the Data on Sam’s Phone.

The government underscores what Sam does not argue in his motion – he does not challenge the search incident to his arrest that located the cell phone on his person, or the seizure of the phone. And to be clear, at no time did law enforcement search the communications on the phone or the data stored on it, such as call logs, contact lists, photographs, or videos. Instead, law enforcement merely viewed the publicly accessible information displayed on the phone’s lock screen, which included the nickname “STREEZY” written across the screen. Yet Sam argues that law enforcement’s knowledge of the nickname “STREEZY” displayed on the lock screen – presumably admitted at trial through the testimony of a law enforcement officer or the admission of the photograph depicting the lock screen – must be suppressed as an illegal search because it was obtained without a warrant. Sam’s motion relies on the Supreme Court’s decision in *Riley v. California*, 573 U.S. 373 (2014) to support its argument, but the Supreme Court’s discussion in *Riley* actually leads to the opposition conclusion.

Riley involves two cases consolidated for appeal to answer one common question: “whether the police may, without a warrant, search digital information on a cell phone seized from an individual who has been arrested.” *Riley*, 573 U.S. at 378. In the first case, law enforcement had seized a smart phone from the defendant’s pants pocket and first went through the phone noting that some words (presumably in the phone’s contacts list or text messages) were preceded by the letters “CK,” a slang label used for members of the Bloods gang. Law enforcement later further examined the contents of the phone, including photographs and videos, all without a warrant. *Id.* at 379. In the second case, law enforcement had seized a flip phone from the defendant, which displayed the words “my house” on the phone’s external screen every time the phone rang. The police opened the phone and saw a picture of a woman and baby set as the phone’s internal wallpaper. They then accessed the phone’s call log, as well as hit a button to determine the phone number associated with the “my house” label. Finally, they used an online phone directory to trace that phone number to an apartment building, at which they identified a woman by her picture

1 on the phone, obtained a warrant to search her apartment, and found drugs and firearms. The
 2 defendant moved to suppress this evidence as fruit of the unconstitutional search of his
 3 phone. *Id.* at 380. In its consolidated decision, the Supreme Court held that officers “must
 4 generally secure a warrant before conducting such a search [of data on cell phones].”

5 Accordingly, Sam is correct that law enforcement is required to obtain a search
 6 warrant prior to conducting a search for data on a cell phone. The real question, then, is
 7 what constitutes a search for data. To answer this question, in *dicta* the *Riley* court provided
 8 numerous examples of what does not qualify as a search for data. Specifically, the Court
 9 provided the following examples of things law enforcement can do with a cell phone without
 10 a warrant:

- 11 • “Law enforcement officers remain free to examine the physical aspects of a
 12 phone to ensure it will not be used as a weapon. . .” *Id.* at 387.
- 13 • Law enforcement officers can also take steps to prevent remote wiping,
 14 including by turning the phone off or removing its battery. *Id.* at 390.
- 15 • “[I]f officers happen to seize a phone in an unlocked state, they may be able to
 16 disable [the] phone’s automatic-lock feature in order to prevent the phone from
 17 locking and encrypting data.” *Id.* at 391.

18 Based on these examples, it is clear that officers are permitted to touch buttons on a phone –
 19 thereby potentially causing the phone to display a background screen or lock screen in plain
 20 view – in order to prevent the potential destruction of evidence, without first obtaining a
 21 warrant. *See also United States v. Pacheco*, No. 11CR121-A, 2015 WL 3402832, *6
 22 (W.D.N.Y. May 25, 2017) (approving of tactile means to turn a phone on prior to obtaining a
 23 warrant, as well as officers’ warrantless removal of the back plate of phones and removal of
 24 phone batteries in order to look for serial numbers). This is true because individuals do not
 25 have a reasonable expectation of privacy over the lock screens on their phone. Given that
 26 the Supreme Court has approved of officers pressing buttons to turn phones off and pressing
 27 buttons to turn off a phone’s auto-lock feature (which, on most smartphones, would
 28

1 illuminate the background or lock screen), it cannot be the case that the agent's pressing of
2 the power button and viewing of the lock screen here would constitute a warrantless search.

3 In his motion, Sam cites only one case other than *Riley*, but that case does not support
4 his position. In *United States v. Lopez-Cruz*, 730 F.3d 803 (9th Cir. 2013), the defendant had
5 consented to allow officers to "look in" and "search" his cell phone, but had not consented to
6 the officers answering the phone when it rang, pretending to be him, or engaging in
7 conversation with the callers, but that is exactly what happened on three separate occasions.
8 Thus, the question the Ninth Circuit examined was the scope of the defendant's consent.
9 The Court answered this by holding as follows: "the agent's answering of the phone
10 exceeded the scope of the consent that he obtained and, thus, violated Lopez's Fourth
11 Amendment rights. As a general matter, consent to search a cell phone is insufficient to
12 allow an agent to answer that phone; rather, specific consent to answer is necessary." *Id.* at
13 811.

14 In the present case, the officers' actions are akin to what occurred in *Pacheco* and
15 what the Supreme Court described in *dicta* in *Riley*, not to the answering of phones without
16 consent as in *Lopez-Cruz*. Indeed, all that occurred here is that officers pressed the power
17 button to wake the phone out of its sleep mode (it was already turned on), which then
18 showed the lock screen and the nickname "STREEZY" displayed across the screen, over
19 which Sam did not have a reasonable expectation of privacy. Officers did nothing more –
20 they did not search through call logs, contact lists, photographs, videos, communications, or
21 anything else. Nor did they answer the phone and pretend to be Sam. This was not a
22 warrantless search for data prohibited by *Riley*, but a simple touching of the power button
23 that displayed words not even protected by the lock feature on the phone. As such, *Riley*
24 does not compel suppression here.

25 //

26 //

27 //

1 **III. CONCLUSION**

2 For the reasons set forth above, the United States respectfully requests that the Court
3 deny Sam's Motion to Suppress Cell Phone Contents.

4 DATED this 20th day of March, 2010.

5
6 BRIAN T. MORAN
7 United States Attorney

8
9 s/ Rebecca S. Cohen
10 REBECCA S. COHEN
11 J. TATE LONDON
12 Assistant United States Attorneys
13 United States Attorney's Office
14 700 Stewart Street, Suite 5220
15 Seattle, Washington 98101-1271
16 Phone: (206) 553-7970
17 E-mail: Rebecca.Cohen@usdoj.gov
18
19
20
21
22
23
24
25
26
27
28

CERTIFICATE OF SERVICE

I hereby certify that on March 20, 2020, I electronically filed the foregoing with the Clerk of Court using the CM/ECF system which will send notification of such filing to the attorneys of record for the defendant.

s/ Rebekah Pfrimmer
REBEKAH PFRIMMER
Legal Assistant
United States Attorney's Office
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
Phone: (206) 553-7970
E-mail: Rebekah.Pfrimmer@usdoj.gov